Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat
Francois Le Coat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1528 07/19/13

~ S Korea Accuses N Korea ~ People Are Talking! ~ Coalition Sues NSA!
~ How Microsoft Aided NSA ~ Congress Needs Lesson! ~ Aniplayer 2.23 Out!

~ Yahoo Turnaround Doubts ~ Network Solutions Hack ~ Surface Is Disaster!
~ Taiwan A Testing Ground ~ Florida Cops Nab Idiot ~ War On PC Bloatware!

-* Surveillance Disclosures Urged *-
-* Gamers Can't Handle New Female Head *-
-* Secret Court Sides With Yahoo in PRISM Case *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

It's like Day 6 for this current heat wave; temps reaching 97 here in the Northeast today, with the heat index well over 100! At least one more day in the 90's is forecast. Whoever said it ain't the heat, but the humidity, was wrong - it's both!

I don't know how those that have to work outside under these conditions manage to do it. My hat is off to those people, however. I brought my car to the mechanic today to get some work done; I didn't realize that the large garage isn't air-conditioned. I know that they closed early today because of the heat. Some people just can't "call it a day" because of the weather.

Speaking of the heat, Rolling Stone magazine is certainly taking some heat these days for their latest cover featuring one of the Boston Marathon bombing suspects. Really? They couldn't produce a cover that tastefully portrayed the victims and/or heroes of that fateful day? That cover gave me the impression that they were glorifying this terrorist, not depicting someone who falls into the readership age bracket and led a troubled life. Sorry, Rolling Stone, but you blew it big time.

And, unfortunately, there is likely going to be some fallout from this because of the negative reactions to the cover. It seems a Massachusetts State Trooper released some photographs of the [alleged] terrorist that were taken at the scene where he was finally captured. Some of the photos showed the suspect covered in blood. Some showed stils of a sharpshooter's laser-directed targeting of the suspect. The trooper's goal was to depict images of the "real" person from that day, not some image typical of a glorified rock star. I sympathise with the trooper, but I don't think that he should have released those photos. Yet another "victim" from this horrific event in Boston history.

Until next time...

=~=~=~=

Hi,

Read on <http://firebee.org/> the last week-end.

New official Aniplayer Version published

This weekend - for the first time since 2004 - a new version of the multimedia player Aniplayer by Didier MØquignon got published. Aniplayer can be described as the most known player for Atari systems. Beside many news for Clones, upgrade cards etc. there is especially one feature of high interest for the FireBee : the MPEG audio decoding uses now the Coldfire MAC instructions. This means nothing else than MPEGs can be played with low system load (even in the background) by Aniplayer.

Have fun with the now official version 2.23 of Aniplayer !

<http://aniplay.atari.org>

=~=~=~=

->In This Week's Gaming Section - Gamers Can't Handle New Female Head at Xbox!

"""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

"""""""""""""""""""""""""""""""""""""

Gamers Can't Handle the New Female Head at Xbox

Microsoft's new company reorganization promotes Julie Larson-Green, a 19-year company veteran, to head up Xbox a position recently left vacant by Don Mattrick a move that has a lot of gamers very, very upset because she's a woman, who supposedly has no gaming experience. Oh and also, she's hot. When the news hit the social gaming news site N4G, commenters were quick to point out her shortcomings, emphasis noted by "games freak" and journalist Lauren Wainwright.

The type is a bit small, but one of the underlined parts suggests that Larson-Green will create terrible games "dedicated to baking and knitting." Though another calms that person down noting that she's "just another figurehead. Easy on the eyes, too." Over at Gamespot we get a lot more on her physical appearance. "Love to get her in front of the Kinect spycam," "milf," and "JLG > Helen Mirren" are the top three comments.

Further down, though, someone counters with: "why cant they get someone hotter... she looks old and wrinkly." This standard gamer talk is all particularly amusing in this situation since, Larson-Green is ultimately in charge of making the sexist gamers' games (i.e. crack), which is kind of like a drug addict disapproving of their female drug dealer because of her gender.

Of course her looks and chromosomal makeup have nothing to do with her ability to lead Xbox, and neither does her vast experience within the company, as chronicled by Wired's Ryan Tate, apparently. Beyond the whole female part of her genetic make-up, the gaming community also won't accept her, both because she has no video game-industry experience and also because she isn't a "gamer." Redditors are up in arms over Larson-Green's new role because she's not One of Them. "Somebody's extensive history and love for the video game industry has a direct relation to how a game console is ultimately developed," writes Redditor SyrioForel.

It's not clear how much Larson-Green does or does not love the gaming industry, however. Assuming she doesn't love video games comes off as sexist, argues Wainwright. (Would people jump to say that about a dude? Wainwright suggests not.) Someone in Larson-Green's position probably doesn't have as much time for hardcore gaming as people commenting in video game websites. But, it's also not clear how much loving games, or even gaming-specific industry experience matters for success. There are plenty of examples of success and failure in the gaming world from all sorts of figures, as pointed out by one dissenting N4G commenter. "A good example is Peter Moore, before working at Sega and subsequently MS, he actually worked at Rebook."

Plus, having a woman at the helm could have other benefits for the notoriously sexist gaming industry. Maybe some baking and knitting games would make women feel a bit more welcome in a world known for its sexual harassment, rape jokes, and general derision of "fake geek girls."

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Apple, Google, Dozens of Others Urge Surveillance Disclosures

Dozens of companies, non-profits and trade organizations including Apple Inc, Google Inc and Facebook Inc sent a letter Thursday pushing the Obama administration and Congress for more disclosures on the government's national security-related requests for user data.

Together with LinkedIn Corp, Yahoo! Inc, Microsoft Corp, Twitter and many others, the companies asked for more transparency of secret data gathering in the letter addressed to President Barack Obama, Attorney General Eric Holder, National Intelligence Director James Clapper, National Security Agency (NSA) Director General Keith Alexander and national security leaders in Congress.

Tech companies have been scrambling to assert their independence after documents leaked last month by former U.S. security contractor Edward Snowden suggested they had given the government direct access to their computers as part of the NSA’s secret surveillance program called Prism.

Such data collection activities are overseen by the secretive Foreign Intelligence Surveillance Court and largely done under the laws of the U.S. Foreign Intelligence Surveillance Act (FISA) and the USA PATRIOT Act.

The classified nature of the data gathering has barred the participating companies from disclosing even their involvement, let alone the content of the requests.

The leaks have renewed a public debate over the balance between national security and privacy, and have put tech companies in an awkward position, especially because many have been assailed for their own commercial use of customer data.

Some companies, including Facebook and Apple, in June struck an agreement with the government to release some information about the number of surveillance requests they receive. But they were limited to disclosing aggregate government requests for data without showing the split between surveillance and criminal requests, and only for a six-month period.

In Thursday’s letter, they asked to be allowed to regularly report statistics on the number and scope of user data requests done under specific national security authorities and the number of individuals, accounts or devices affected by those requests.

"This information about how and how often the government is using these legal authorities is important to the American people, who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of U.S.-based service providers who are concerned about the privacy and security of their communications," the letter said.

The letter also asked Congress to pass legislation that would require the federal government to make transparency reports and let companies disclose user data requests without having to first ask the FISA Court for permission.

Co-signers included investors such as Boston Common Asset management and Union Square Ventures, as well as scores of associations including Human Rights Watch, Electronic Frontier Foundation, American Civil Liberties nion, Americans for Tax Reform and conservative FreedomWorks.

One of the lawmakers the letter was addressed to is Senate Judiciary Committee Chairman Patrick Leahy, a Democrat who has introduced a bill that would expand reporting requirements for the secret programs, add more court reviews and move up the expiration of the authorization for some of the data collection by 2-1/2 years.

"Americans deserve to know how much of their communications data is being swept up by government surveillance, and the government’s use of these authorities must be subject to strong oversight," Leahy said on Thursday.

He said the Judiciary Committee will hold another hearing on the issue later this month.

The U.S. government is facing multiple court challenges over its surveillance programs. Yahoo this week scored a victory when the FISA Court sided with the Internet company and ordered the Obama administration to declassify and publish a 2008 court decision justifying the Prism program.

The government is expected to decide by August 26 which parts of the 2008 opinion may be published, according to a separate court filing by the Justice Department.

The White House and the Department of Justice did not immediately comment on Thursday’s letter.

Secret Court Sides with Yahoo, Orders U.S. To Declassify Prism Surveillance Ruli ng

A secret U.S. court overseeing government domestic surveillance activities has sided with Yahoo Inc and ordered the Obama administration to declassify and publish a 2008 court decision justifying Prism, the data collection program revealed last month by former security contractor Edward Snowden.

The ruling could offer a rare glimpse into how the government has legally justified its spy agencies’ data collection programs under the Foreign Intelligence Surveillance Act (FISA).

Judge Reggie Walton of the Foreign Intelligence Surveillance Court issued Monday’s ruling. The government is expected to decide by August 26 which parts of the 2008 opinion may be published, according to a separate court filing by the Justice Department.

Controversial U.S. data collection activities are overseen by the Foreign Intelligence Surveillance Court and its appeals body, the Foreign Intelligence Surveillance Court of Review. Both have been shrouded in secrecy since their creation more than three decades ago.

The 2008 ruling stemmed from Yahoo’s challenge of the legality of broad, warrantless surveillance programs like Prism.

In June, after Snowden leaked information about Prism to the Washington Post and the Guardian newspapers, Yahoo’s lawyers asked the courts and government to declassify and publish decisions upholding the constitutionality of the program.

Legal experts who follow surveillance cases said the 2008 ruling may not reveal any strikingly novel legal reasoning by the government or the courts. But civil liberties advocates said the significance of the ruling may lie in the court’s decision itself to declassify the previously secret 2008 ruling.

"Unless the public knows what the laws mean, it can’t really assess how much power (it has) given its government," said Patrick Toomey, a national security fellow at the American Civil Liberties Union.

Monday’s ruling "is a suggestion that the FISA court is primed now to consider the government’s assertion of the necessity of secrecy," Toomey said. "It’s a promising first step."

The decision is also a victory for Yahoo Inc, which said in a statement on Tuesday that it was "very pleased" with the court's ruling.

"Once those documents are made public, we believe they will contribute constructively to the ongoing public discussion around online privacy," Yahoo said.

Other Internet companies, including Google Inc and Facebook Inc, began participating in Prism in early 2009 soon after Yahoo lost its appeal before the Foreign Intelligence Surveillance Court of Review.

It is not known if Yahoo, or any other party, has sought to appeal to the U.S. Supreme Court.

A number of major U.S. Internet companies, including Microsoft, Google and Facebook have asked the government for permission to disclose the number of national security-related user data requests they receive.

On Tuesday, Microsoft published an lengthy letter to U.S. Attorney General Eric Holder asking for greater freedom to publicly discuss how it turns over user information to the government. The letter was a response to a Guardian report that said Microsoft had given authorities the ability to circumvent encryption of Outlook emails and to capture Skype online chats. Microsoft has contested the report, saying it has "significant inaccuracies.

Until recent weeks, Yahoo was prohibited from discussing its activities in the secret courts or even acknowledging the existence of its legal challenge.

The decision to release the 2008 ruling comes as Snowden remained at a Moscow airport, awaiting political asylum. On Tuesday, he applied for asylum in Russia.

In the coming weeks, the government is expected to publish the lower FISA court's 2008 ruling in the Yahoo case and legal briefs related to it. In an uncommon move, the U.S. had previously agreed to declassify a heavily redacted version of the appeals court ruling in the case.

The government has long argued on the grounds of national security that the surveillance courts' proceedings must be secret. Public and political reaction to Snowden's revelations has put pressure on that position.

In June, Senators Jeff Merkley, a Democrat from Oregon, and Mike Lee, a Utah Republican, introduced a bill that would require the government to declassify significant court rulings concerning the FISA court and its supervision of secret wiretapping programs.

"Americans deserve to know how much information about their private communications the government believes it's allowed to take under the law," Merkley said.

How Microsoft Handed The NSA Access to Encrypted Messages

Microsoft has collaborated closely with US intelligence services to allow users' communications to be intercepted, including helping the Nationa

Security Agency to circumvent the company’s own encryption, according to top-secret documents obtained by the Guardian.

The files provided by Edward Snowden illustrate the scale of co-operation between Silicon Valley and the intelligence agencies over the last three years. They also shed new light on the workings of the top-secret Prism program, which was disclosed by the Guardian and the Washington Post last month.

The documents show that:

- Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal;

- The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail;

- The company worked with the FBI this year to allow the NSA easier access via Prism to its cloud storage service SkyDrive, which now has more than 250 million users worldwide;

- Microsoft also worked with the FBI’s Data Intercept Unit to "understand" potential issues with a feature in Outlook.com that allows users to create email aliases;

- In July last year, nine months after Microsoft bought Skype, the NSA boasted that a new capability had tripled the amount of Skype video calls being collected through Prism;

- Material collected through Prism is routinely shared with the FBI and CIA, with one NSA document describing the program as a "team sport".

The latest NSA revelations further expose the tensions between Silicon Valley and the Obama administration. All the major tech firms are lobbying the government to allow them to disclose more fully the extent and nature of their co-operation with the NSA to meet their customers’ privacy concerns. Privately, tech executives are at pains to distance themselves from claims of collaboration and teamwork given by the NSA documents, and insist the process is driven by legal compulsion.

In a statement, Microsoft said: "When we upgrade or update products we aren’t absolved from the need to comply with existing or future lawful demands." The company reiterated its argument that it provides customer data "only in response to government demands and we only ever comply with orders for requests about specific accounts or identifiers".

In June, the Guardian revealed that the NSA claimed to have "direct access" through the Prism program to the systems of many major internet companies, including Microsoft, Skype, Apple, Google, Facebook and Yahoo.

Blanket orders from the secret surveillance court allow these communications to be collected without an individual warrant if the NSA operative has a 51% belief that the target is not a US citizen and is not on US soil at the time. Targeting US citizens does require an individual warrant, but the NSA is able to collect Americans’ communications without a warrant if the target is a foreign national located overseas.

Since Prism’s existence became public, Microsoft and the other companies listed on the NSA documents as providers have denied all knowledge of the program and insisted that the intelligence agencies do not have back doors into their systems.

Microsoft’s latest marketing campaign, launched in April, emphasizes its commitment to privacy with the slogan: "Your privacy is our priority."

Similarly, Skype’s privacy policy states: "Skype is committed to respecting your privacy and the confidentiality of your personal data, traffic data and communications content."

But internal NSA newsletters, marked top secret, suggest the co-operation between the intelligence community and the companies is deep and ongoing.

The latest documents come from the NSA’s Special Source Operations (SSO) division, described by Snowden as the "crown jewel" of the agency. It is responsible for all programs aimed at US communications systems through corporate partnerships such as Prism.

The files show that the NSA became concerned about the interception of encrypted chats on Microsoft’s Outlook.com portal from the moment the company began testing the service in July last year.

Within five months, the documents explain, Microsoft and the FBI had come up with a solution that allowed the NSA to circumvent encryption on Outlook.com chats

A newsletter entry dated 26 December 2012 states: "MS [Microsoft], working with the FBI, developed a surveillance capability to deal" with the issue. "These solutions were successfully tested and went live 12 Dec 2012."

Two months later, in February this year, Microsoft officially launched the Outlook.com portal.

Another newsletter entry stated that NSA already had pre-encryption access to Outlook email. "For Prism collection against Hotmail, Live, and Outlook.com emails will be unaffected because Prism collects this data prior to encryption."

Microsoft’s co-operation was not limited to Outlook.com. An entry dated 8 April 2013 describes how the company worked "for many months" with the FBI which acts as the liaison between the intelligence agencies and Silicon Valley on Prism to allow Prism access without separate authorization to its cloud storage service SkyDrive.

The document describes how this access "means that analysts will no longer have to make a special request to SSO for this a process step that many analysts may not have known about".

The NSA explained that "this new capability will result in a much more complete and timely collection response". It continued: "This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established."

A separate entry identified another area for collaboration. "The FBI Data Intercept Technology Unit (DITU) team is working with Microsoft to understand an additional feature in Outlook.com which allows users to create email aliases, which may affect our tasking processes."

The NSA has devoted substantial efforts in the last two years to work with Microsoft to ensure increased access to Skype, which has an estimated 663 million global users.

One document boasts that Prism monitoring of Skype video production has roughly tripled since a new capability was added on 14 July 2012. "The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture'," it says.

Eight months before being bought by Microsoft, Skype joined the Prism program in February 2011.

According to the NSA documents, work had begun on smoothly integrating Skype into Prism in November 2010, but it was not until 4 February 2011 that the company was served with a directive to comply signed by the attorney general.

The NSA was able to start tasking Skype communications the following day, and collection began on 6 February. "Feedback indicated that a collected Skype call was very clear and the metadata looked complete," the document stated, praising the co-operation between NSA teams and the FBI. "Collaborative teamwork was the key to the successful addition of another provider to the Prism system."

ACLU technology expert Chris Soghoian said the revelations would surprise many Skype users. "In the past, Skype made affirmative promises to users about their inability to perform wiretaps," he said. "It's hard to square Microsoft's secret collaboration with the NSA with its high-profile efforts to compete on privacy with Google."

The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies.

The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that "enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism".

The document continues: "The FBI and CIA then can request a copy of Prism collection of any selector " As a result, the author notes: "these two activities underscore the point that Prism is a team sport!"

In its statement to the Guardian, Microsoft said:

> We have clear principles which guide the response across our entire company to government demands for customer information for both law enforcement and national security issues. First, we take our commitments to our customers and to compliance with applicable law very seriously, so we provide customer data only in response to legal processes.
>
> Second, our compliance team examines all demands very closely, and we reject them if we believe they aren't valid. Third, we only ever comply with orders about specific accounts or identifiers, and we would not respond to the kind of blanket orders discussed in the press over the past few weeks, as the volumes documented in our most recent disclosure clearly illustrate.
>
> Finally when we upgrade or update products legal obligations may in

some circumstances require that we maintain the ability to provide information in response to a law enforcement or national security request. There are aspects of this debate that we wish we were able to discuss more freely. That’s why we’ve argued for additional transparency that would help everyone understand and debate these important issues.

In a joint statement, Shawn Turner, spokesman for the director of National Intelligence, and Judith Emmel, spokeswoman for the NSA, said:

The articles describe court-ordered surveillance and a US company’s efforts to comply with these legally mandated requirements. The US operates its programs under a strict oversight regime, with careful monitoring by the courts, Congress and the Director of National Intelligence. Not all countries have equivalent oversight requirements to protect civil liberties and privacy.

They added: "In practice, US companies put energy, focus and commitment into consistently protecting the privacy of their customers around the world, while meeting their obligations under the laws of the US and other countries in which they operate."

Broad Coalition Sues NSA Over ’Illegal’ Telephone Surveillance Dragnet

A diverse coalition of 19 groups announced today a lawsuit against the United States government for "an illegal and unconstitutional program of dragnet electronic surveillance," known as the Associational Tracking Program, which collects all telephone records handled by Verizon, AT&T, and Sprint in the US. The group, represented by the Electronic Frontier Foundation, aims to compel the government to inventory and disclose the records in its possession, to destroy them, and to immediately end the surveillance program.

"The bulk collection of telephone communications information without a valid, particularized warrant supported by probable cause violates the First, Fourth, and Fifth Amendments, as well as statutory prohibitions and limitations on electronic surveillance," the suit alleges. "The program collects information concerning all calls wholly within the United States, including local telephone calls, as well as all calls between the United States and abroad, regardless of a connection to international terrorism, reasonable suspicion of criminality, or any other form of wrongdoing."

""The bulk collection violates the First, Fourth, and Fifth Amendments.""

The surveillance program was revealed on June 6th when The Guardian reported that Verizon has been amassing metadata records on every telephone call made in the country over the past seven years. The Wall Street Journal quickly corroborated that report, and confirmed that AT&T and Sprint have also been involved in the NSA’s telephone data collection program. The program is enabled by Section 215 of the Patriot Act: a controversial law that allows the government to conduct surveillance based on broad warrants for a wide variety of records, even if there is no connection to terrorism.

The coalition filing suit today joins other groups that are challenging the program, including the Electronic Privacy Information Center and the American Civil Liberties Union. But so far, resistance to the

government’s surveillance programs have not fared well in courts.

The suit is represented by a diverse coalition, including Public Knowledge, the Open Technology Institute, Free Press, Greenpeace, Human Rights Watch, the First Unitarian Church of Los Angeles, the Council on Islamic Relations, the California Association of Federal Firearms Licensees, Media Alliance, and the National Organization for the Reform of Marijuana Laws. The Verge will continue to follow these suits as they develop; as Wired notes, the government has yet to respond to the allegations in court.

Plunging Ad Prices Underscore Doubts Over Yahoo Turnaround Plan

Marissa Mayer’s plan to resuscitate Yahoo seems a simple one: get back the eyeballs, sell more ads and charge higher prices. But the chief executive’s plan seems to have run into a major snag.

The price the company charges per ad slid 12 percent in the April to June period, six times the decline just a quarter ago - a fall that some say highlights how Yahoo has been caught unprepared for the industry shift to automated, programmatic ad buying.

Marketers increasingly prefer to buy online advertising space through automated exchanges, where prices are significantly lower, rather than paying top-dollar for premium ads sold by a Web publisher’s salesforce. Ads offered by exchanges also allow marketers to aim ads in real time at specific audiences, such as by gender or age.

Yahoo’s ad focus has, however, centered on "on developing media units that were much better for premium buys," said Shar VanBoskirk, an analyst with industry research firm Forrester Research.

Yahoo has its own programmatic ad technology with its Right Media exchange. But analysts say the exchange is not as popular as rival offerings, such as Google’s DoubleClick exchange, which is considered the industry standard.

Google, the world’s No.1 Web search engine, will report its second-quarter earnings on Thursday.

For many on Wall Street, the industry shift is one more reason means Yahoo’s turnaround remains "an open question", especially given that Mayer has said the company remains first and foremost an advertising company.

During Tuesday’s post-earnings conference call with analysts, Mayer said Yahoo was bullish on its advertising technology and that it planned to focus on improving various aspects of it in the coming quarters.

But even if Yahoo’s ad exchange becomes more competitive, the broader trend of programmatic advertising will continue to pressure its business.

"Programmatic advertising technology continues to have a downward bias to pricing in display advertising and I don’t expect that to improve anytime soon," said UBS analyst Eric Sheridan.

Mayer took the reins at Yahoo in July 2012 after a tumultuous period in which the company churned through several CEOs and many of its top

executives and engineers jumped ship.

She has revamped key products such as mail and the Yahoo home page and jumpstarted acquisitions. Last month, Yahoo closed its $1.1 billion acquisition of popular blogging service Tumblr.

Yahoo’s stock has surged roughly 70 percent since Mayer took the helm but much of the gain has come from stock buybacks and from Yahoo’s Asian assets, including a 24 percent stake in Chinese e-commerce giant and potential IPO debutante Alibaba Group.

Ad numbers, however, remain dismal. Apart from pricing, display ad volumes and paid-clicks for search ads - an important measure of viewers and readers’ responsiveness to marketing - continue to shrink.

Yahoo’s share of the $17 billion U.S. display ad market is expected to decline to 7.9 percent in 2013, down from a 9.2 percent share last year, while Google’s share is expected to grow to 17.6 percent. Facebook is likely to expand its market share to 16.5 percent, research house eMarketer estimates.

"This core business is going to be ugly for quite some time before it gets better," BGC analyst Colin Gillis said of Yahoo.

"This is just the beginning of the trend, of the drop in the price per ad. You still have a pretty big gap between what you can get direct and what you can get selling on an exchange."

Hacking Attack Blamed for Network Solutions Outage

Network Solutions says a hacking attack is causing service disruptions that are affecting its website customers.

The company’s Facebook page offers few details, but the company says it’s facing a distributed denial of service attack in which hackers direct thousands of computers to access a website all at once. The fake traffic makes it difficult for legitimate visitors to get through.

Network Solutions Inc. registers domain names and provides computers and other technologies to host websites for companies, groups and individuals. Some sites, including Network Solutions’ home page, may be slow or inaccessible as a result of the attack.

Wednesday’s Facebook post says Network Solutions’ technology team is working to mitigate the impact of the attack.

The duration of the attack and the extent of damages were not immediately clear.

South Korea Accuses North of Cyber Attacks

South Korea accused North Korea on Tuesday of mounting cyber attacks on the websites of its presidential office and other government agencies, saying it had identified signature malicious computer codes and an

internet address.

The cyber attacks took place last month, on the anniversary of the beginning of the 1950-53 Korean War which left the peninsula divided between the rival countries.

North Korea has been suspected of masterminding previous cyber attacks on South Korea, including one in March that paralyzed tens of thousands of computers and servers at major broadcasters and banks.

North Korea has repeatedly denied responsibility for such attacks saying it has also been a victim of hacking.

South Korean officials said they had detected North Korean involvement in the latest cyber assault that shut down several sites including those of the presidential office and the conservative ruling party.

"An IP address within North Korea's bandwidth was found," Chun Kilsoo, an official at the state-run Korea Internet and Security Agency, told a briefing, referring to a computer's internet protocol address.

The malicious computer codes and technique of the attack were similar to those detected in previous hacking attacks traced to the North, officials added.

The accusation comes as the two Koreas wrangle over the reopening of a joint factory park just inside North Korea that North Korea closed during a period of tension that began when it conducted its third nuclear test in February.

They failed to reach agreement on Monday on the reopening of the complex.

South Korea has not confirmed findings by U.S. online security company McAfee that a group of hackers was behind a string of cyber attacks on South Korea dating back to 2009 aimed at spying on its military.

South Korea's defense minister said at a recent conference that North Korea had about 3,000 highly trained cyber warfare personnel, according to media reports.

In March, the North suggested the United States was behind cyber attacks on its internet servers after reports of disruptions to its main news services.

A hacker collective known as Anonymous said it had attacked North Korean websites on the anniversary of the Korean War.

The group denied through Twitter posts any involvement in attacks on South Korea.

Taiwan A 'Testing Ground' for Chinese Cyber Army

Taiwan is the frontline in an emerging global battle for cyberspace, according to elite hackers in the island's IT industry, who say it has become a rehearsal area for the Chinese cyberattacks that have strained ties with the United States.

The self-governing island, they say, has endured at least a decade of highly-targeted data-theft attacks that are then directed towards larger countries.

"We've seen everything," said Jim Liu, the 28-year-old founder of Lucent Sky, a Taiwanese internet security company specializing in resolving dangerous software vulnerabilities that hackers can exploit in order to gain access to a system.

"We'll see a specific attack signature here, and then six months later see the same signature in an attack on the States."

A Pentagon report in May accused China of trying to break into U.S. defense computer networks. It followed another report in February by U.S. computer security company Mandiant that said a secretive Chinese military unit was probably behind a series of hacking attacks that had stolen data from 100 U.S. companies.

Beijing dismissed both reports as without foundation. But Taiwan experts say that hacking methods such as those outlined in the Mandiant report are the same kinds of security breaches that they had seen several years earlier.

Regarded by China as a renegade province it must recover, by force if necessary, it is easy to see why Taiwan might be an ideal target for Chinese hackers: it is close to the mainland, Mandarin-speaking and boasts advanced internet infrastructure.

This cyber war playing out across the narrow Taiwan Strait first came to public attention in 2003, when a Taiwanese police agency realized hackers had stolen personal data, including household registration information, from its computer system.

These attacks differed from traditional hacking attempts - where many casual hackers attempt to disrupt their targets' systems, these hackers went in stealthily, with the intention to plunder rather than destroy.

"Back then it was very rare to see these kinds of social network attacks," said hacking specialist Jeremy Chiu, a contract instructor in IT for Taiwan's intelligence agencies. "They were very, very well organized."

Other indicators, including the ease with which the hackers penetrated an email system written entirely in Chinese, painted a picture of the culprits as a large, coordinated group of mainland Chinese hackers.

"One thing that indicates government support for these attacks is just the sheer volume - how many agencies are being attacked on a daily basis," said Benson Wu, postdoctoral researcher in information technology at Taiwanese think-tank Academia Sinica and co-founder of Xecure Lab, which focuses on responding to advanced persistent threats.

Interviewed at his downtown Taipei office, Wu's set-up fits the classic hacker image: dimly-lit, strewn with wires and humming with computers.

On a projector screen he displayed a list of emails, written in Chinese, with subject headings like "meeting notes", "dinner attendance" and "questionnaire".

"These are all hacking attempts," Wu explained. Once the documents have been opened, they plant a backdoor allowing the hacker virtually

unfettered access to the network.

One such "spearphishing" attack was reportedly used on the White House in October. A Taiwan expert in cyberespionage interviewed by Reuters estimated that thousands of Taiwanese high-level government employees receive as many as 20 to 30 of these emails a month.

"We've been following these Chinese hackers for so long, we can track their daily work schedule," said the expert, who asked not to be identified.

"People expect hackers to be night owls, but these guys work very normal hours - on Chinese national holidays, for example, we don't see any hacking activity at all."

Tracking the exact source of the attacks, however, remains a slippery game of internet sleuth.

"We take the IP address culled from the attack as a springboard, then track it through the internet - perhaps the same IP address was used in a forum registration, or to register a QQ handle," he said, referring to a popular Chinese chat program. "It depends how good they are at covering their tracks."

China denies being behind hacking attacks on other nations and insists it is a major victim of cyber attacks, including from the United States - an argument that Beijing sees as strengthened by revelations last month from a former National Security Agency contractor, Edward Snowden, about top-secret U.S. electronic surveillance programs.

The United States and China held talks focused on cyber issues last week.

According to internet platform Akamai, 27 percent of worldwide hacking activity during 2012 originated in China. The same report, however, also placed Taiwan among the top five digital attack originating countries in 2012.

"Taiwan is one of the key countries where we see a lot of activity," said Singapore-based malware researcher Chong Rong Hwa of network security firm FireEye Inc.

A report issued by SecureWorks, a network safety arm of PC maker Dell Inc, said Taiwan government ministries are swarming with a particularly malicious form of data-nabbing computer virus.

In one year, the Taiwan National Security Bureau encountered more than 3 million hacking attempts from China, according to statements given by bureau director Tsai Teh-sheng in March in response to questions from lawmakers.

Military and technology intelligence was included among the pilfered data. A representative from the bureau declined to comment when contacted by Reuters.

"Taiwan will continue to be the battleground for lots of cyber attacks; it's like we are on our own," Wu said. "China has a huge pool of talent and technical resources."

Congress Needs A Lesson in Passwords

Anonymous claims to have hacked the emails and passwords of some Congress persons and a bunch of their staffers, revealing that the members of our esteemed government have terrible password habits. The list came via the Anonymous twitter handle OpsLastResort in protest of the NSA domestic spying revelations. The document claims to have the "current valid credentials" of more than 2,000 people. But, out of the kindness of their hearts, they "HAVE REMOVED SOME OF THE PASSWORDS AND SHUFFLED THE ORDER OF THE REMAINING ONES." Even without knowing who chose what password, it's certain that Hill people need a lesson in Internet security, assuming the list is genuine. But, even if the list is fake, it's never too late to brush up on the rules. So, free of charge, here are some tips and tricks for you guys. You're welcome.

Lesson 1: Don't use "congress" in your password. Putting a series of numbers, an exclamation point, or other symbols after the word "congress" does not make it a smart choice. And, yet, 20 people on this list used some iteration of "congress" to protect their government emails. Considering every single person on the list works for Congress and has a house.go or senate.gov email address, the word "congress" is the most obvious choice any reasonably smart hacker would think to search.

Lesson 2: "Republican" or "democrat" is dumb, too. For the same reason as above, the two people on the list who chose their party as their password need to change that. Especially the guy who picked "TX32republican!" Do you happen to work for Pete Sessions, the Republican congressman for Texas's 32nd district? See how easy that was.

Lesson 3: States with numbers are also incredibly obvious. Quite a few people on the list decided to use the state they worked for plus the congressional district number. That's only slightly less obvious than "congress" and makes matching the username to the password even easier, since "California20th" can match up with a very particular House member and all he or she's particular staffers.

Lesson 4: Never, ever use any part of your name. Hey Justine Sessions, is your password #JustineSessions83? On that note, were you born in 1983?

Lesson 5: The 36 people who used "password" as their password probably shouldn't be working for Congress. You guys! Password is the number one most popular, most hackable password on all the Internet. The cardinal rule of password picking is to choose anything but "password" and 12345 putting numbers after the word doesn't make it much harder to guess, either.

Lesson 6: Any real words are a bad idea. To the three people who chose "Starbucks," that's incredibly easy to hack. Hackers often use custom-compiled dictionaries of popular words to guess passwords. If three whole people picked the coffee chain, then it's probably on a hacker list somewhere. To be safe, any real words are bad ideas.

Lesson 7: All your passwords are way too short. To be safe, pick something with 11 or more characters; at that point it gets much, much harder to hack.

Or just keep your terrible passwords; it's not like government email accounts contain any important information or anything.

Florida Cops Nab Suspect Who Posted on Facebook Wanted Poster

A Florida fugitive wanted for robbery helped tip police off to his own whereabouts when he responded to a sheriff’s office Facebook post that included his photograph and warrant.

On July 10, the Pasco County Sherriff’s Office posted a photograph of Matthew Oliver, 23, of New Port Richey, Fla., and asked for information leading to his arrest.

What they got instead was a reply from Oliver himself.

"You guys are going to pay for believing a crackhead and slandering my name," Oliver wrote on the sheriff’s office Facebook page. "Pasco County has nothing but fools investigating crimes for them that’s why these mix up[s] happen."

Oliver went on to say that he was in the hospital during the time of the alleged crime, but when police posted his warrant and asked him to call them, he stopped commenting.

Oliver is wanted for stealing the wallet of a man outside Family Dollar store in December, said Melanie Snow, a spokeswoman for the sheriff’s office.

The sheriff’s office, she said, recently began using Facebook as a "crime-fighting tool," but Oliver was the first suspect to write back.

Oliver’s response helped spread the word, and was shared more than 400 times. That publicity led to the tips cops were hoping for, as people who knew Oliver called police to tell them his whereabouts.

On Friday, as cops were readying to knock on his mother’s door they spotted Oliver outside her home, wearing a camouflage hoodie and promptly arrested him.

He told cops he knew posting on Facebook helped them find him, according to Snow.

Oliver spent the weekend in jail. He has not yet been arraigned.

Microsoft’s Surface RT Launch Was An Absolute and Total Disaster

For one brief, shining night, it appeared that Microsoft’s first tablet would be a success. At a super-surprise press conference in California last June, at which no journalist had any idea what was about to be announced, CEO Steve Ballmer unveiled the Surface, a slick-looking iPad competitor with an innovative kickstand, solid construction and clean Windows 8 software.

It was Microsoft’s first true piece of computing hardware, and the Internet went wild: It was upvoted to the moon on Reddit; millions watched the mesmerizing first advertisement on YouTube; "Shut up and take my money!" was the rallying cry that greeted the Surface on that first night.

It was the kind of reception that is usually reserved for Apple products and the occasional beastly Android phone, but this time - for the first time - a gadget running Microsoft Windows was the rage. Microsoft, for the first time with a product that wasn't a game console, had an honest-to-goodness hit on its hands, and it appeared as though it might actually be able to compete with the iPad and Kindle Fire.

After that night, it seemed like everything fell off a cliff, and then kept rolling and fell off another cliff, beneath which was a bottomless pit: The rollout of the Microsoft Surface was as badly-botched as any product launch I've ever seen. The Internet was shouting "Shut up and take my money," but, astoundingly, Microsoft wouldn't take its money: the company did not announce a price or a release date or a pre-order website for the Surface until an absurd four months after the event; by the time they did, all of the buzz behind the Surface had died down, all of the excitement had fizzled and so many articles had been written dinging the armor of the Surface and questioning its appeal that far fewer wanted to buy one than on the night it came raging out of the darkness. Couple that with a disastrous advertising campaign featuring the cast of Stomp - an ad campaign far less appealing than the teaser commercial above - and the Surface was as doomed as a stick of dynamite.

So we should not be surprised at all that Microsoft just took a $900 million charge on unsold Surface tablets, given just how poorly the launch - which was really more of a slow crawl toward death - went. Not only did it take Microsoft months to announce price and release date and battery life and 4G connectivity - it also chose to sell its tablets exclusively in Microsoft stores, and online through their own site. At the time Microsoft announced this, it had but 20 stores in the entire universe. This is not a good strategy to sell millions of consumer devices worldwide.

The Surface RT is not dead, but given its horrendous beginnings, there will need to be a dramatic turnaround in order for it to be deemed anything but an expensive, ponderous failure. And if Microsoft wants to know why the Surface it's a failure, it shouldn't look at the product itself - which I find totally adequate as a personal tablet - but rather at the launch of the thing itself. It didn't announce a price, it didn't announce a release date and it sold the device at a location that has only now, over a year later, made it to barely over half of the United States.

Microsoft is new at this whole selling-hardware-thing, so it should take a lesson from Apple and Google: When customers want you to shut up and take their money, you should shut up and take their money.

Microsoft Cuts Surface RT Prices, Hopes To Boost Slow Sales

Microsoft's Surface RT is getting price cuts across the world this week as the company looks to boost sales of its first ever tablet hardware. The Verge revealed the price cuts recently for the US, but the cuts are also going into effect in Europe and other international countries that currently offer the Surface RT. Microsoft's online stores and third-party retailers are all offering the tablet at around 30 percent less, with prices varying per region. The software maker is not altering its Surface Pro pricing at this time.

Although Microsoft has entered into the top five vendors for tablet sales worldwide with its Surface devices, the actual sales have been rather slow. IDC recently reported Q1 sales figures for the Surface RT and Surface Pro, totalling just 900,000 with the majority made up of Pro sales. Microsoft is not commenting on Surface sales, and the company has refused to disclose them in its financial reports. Windows CFO Tami Reller has hinted that the company may "provide some updates on how things are going," in future, but there’s little guidance right now.

The price cuts follow a recently launched education program to sell the Surface RT to schools at $199. Microsoft has also been clearing the stock of its Surface RT tablets during its Tech-Ed and Worldwide Partner Conferences, offering them to attendees for just $99. Microsoft is expected to introduce a refreshed Surface RT device, with the company recently hinting at new Surface hardware within the next year.

Startup Wages War on PC Bloatware

One of the more frustrating parts of buying a personal computer comes when you fire it up and realize that the OEM has larded it up with storage-clogging bloatware that degrades your PC s performance. However, startup Jumpshot thinks it has the perfect solution in the form of its USB stick-delivered software that can comb through your PC for little-used software that nevertheless takes up significant resources when you turn on your machine. Once it discovers this apparent bloatware, it removes its icons from your home screen and prevents it from automatically running whenever you switch on your PC. Jumpshot got its start last year as a Kickstarter project that received funding of more than five times its original funding goal.

The Case for Letting Cranky Old Men Hate Twitter

Today the Internet got another one of those trite cases against Twitter, again from someone who doesn’t know how to use Twitter because, this time, he’s not even on the network. These types of columns that come around every so often evoke the same exact foolproof argument against their stupidity: Twitter is what you make it, so it’s your fault if you hate it. The New York Times’s Joe Nocera makes it particularly easy to take down his column with this argument because he admits he doesn’t even use the service. Nocera: You can’t hate Twitter, if you don’t get Twitter. But, this time, maybe it’s time to let the crank-ball hate the terrible digital media thing that "exacerbates our society-wide attention deficit disorder."

Of course, his argument is flawed for all the usual reasons, but Nocera has demonstrated that he has no interest in hearing any constructive criticism of his columns. "If you are mocked on Twitter and you don t know it, have you really been insulted?" he asks. The answer to that rhetorical question in the case of Nocera is no. He doesn’t like Twitter because he doesn’t want to hear mean, or critical, or thoughtful things said about his writing. Even though a column is precisely the kind of journalism that should be a part of discussion. The very kinds of discussions that happen on Twitter every day.

So, there’s really no point in heading on over to Twitter to call him a crank. Or putting up a blog post about his outdated view of the world and then having it tweeted out so that people see and read it. He won’t hear it and doesn’t want to. "Ignorance was bliss," he writes, referring to the time before another @JoeNocera on Twitter started sending him some of the feedback he was missing out on.

Let’s just let the old guy be old and fall into blissful obscurity. Plus, if he’s not on Twitter, we can ignore any and all cranky-old-man things he has to say, confining his columns to a closed system, where only people who seek him out will read him. Imagine if this guy got his hands on an account: Then we’d have to listen to his complaining all day, every day. Totally ignorable column-sized doses are a lot easier to handle.

=~=~=~=